MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2017/2018

TNS3131 – NETWORK SECURITY AND MANAGEMENT

(All sections / Groups)

27 October 2017
9.00 a.m. – 11.00 a.m.
(2 hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages **including cover page with 5 questions only**.

2. Attempt **ALL questions**. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

a) i) Define *active attack* and *passive attack.* [2 marks]
ii) List TWO (2) examples for each type of attacks respectively. [2 marks]

b) Consider an Automated Teller Machine (ATM) in which users provide a Personal Identification Number (PIN) and a card for account access. Give examples of **confidentiality**, **integrity**, and **availability** requirements associated with the system. [3 marks]

c) Define *Specific Security Mechanism*. List TWO (2) examples of specific security mechanisms. [2 marks]

d) Illustrate a secure model for controlled access to information on a computer system in the presence of possible opponents. [3 marks]

QUESTION 2

a) Define TWO (2) criteria to be met if the encryption scheme is said to be computationally secure. [2 marks]

b) Explain the importance of Feistel cipher. List any FOUR (4) design elements of Feistel cipher. [3 marks]

c) Compare DES, Triple DES and AES in terms of key size (bits), block size (bits), number of rounds and possible application for each one of them. [3 marks]

d) Briefly describe FOUR (4) ways public-key can be distributed in public-key cryptography. [4 marks]

QUESTION 3

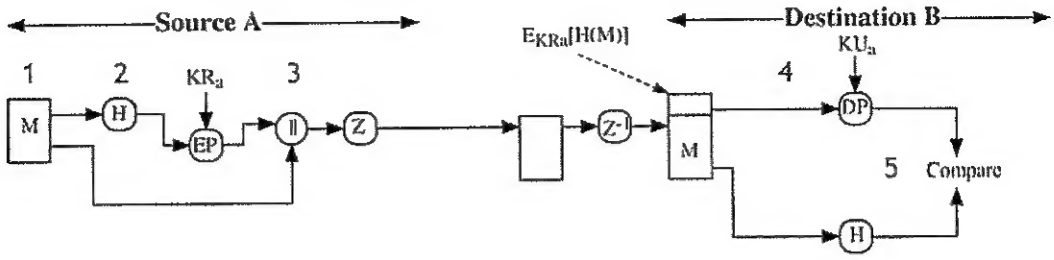
a) List message exchange sequence in Kerberos version 4 and 5. [3 marks]

b) Illustrate the fundamental components of Authentication, Authorization and Accounting (AAA). [3 marks]

c) Given binary input data 00110011 01011100 01010010, identify the character representation for Radix-64 encoding (Refer appendix for Radix-64 table). [3 marks]

Continued ....

d) Given the following illustration for digital signature service provided by Pretty Good Privacy (PGP), describe the numbered 5 steps in the diagram. [3 marks]



QUESTION 4

a) Briefly describe FOUR (4) potential applications of IP security for secured communication across LAN, WAN and Internet. [2 marks]

b) Using the following table, compare the functionality of Authentication Header (AH), Encapsulating Security Payload (ESP) and ESP with authentication in transport mode Security Associations (SA) and tunnel mode SA.

	Transport Mode SA	Tunnel Mode SA
AH		
ESP		
ESP with authentication		

[3 marks]

c) One of the main protections on the web is data integrity.

i. Identify TWO (2) threats under data integrity. [2 marks]
ii. List a consequence of the data integrity threat. [1 mark]
iii. Define a countermeasure for the data integrity threat. [1 mark]

d) Explain TWO (2) important Secure Socket Layer (SSL) concepts. [3 marks]

Continued ....

QUESTION 5

a) Explain FOUR (4) key elements in Simple Network Management Protocol (SNMP). [4 marks]

b) Explain any TWO (2) strategies used in password selection. [2 marks]

c) Explain *salt* and list TWO (2) purposes of salt in the context of UNIX password management. [2 marks]

d) Briefly explain FOUR (4) phases of typical virus or worm operations. [2 marks]

e) In the table format given below, list one advantage and one disadvantage for the listed firewall methods. [2 marks]

Types of Firewalls	**Advantages**	**Disadvantages**
Packet-filtering routers	•	•
Application-level gateways	•	•

Continued ....

Appendix:

Radix-64 table

6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

End of Paper.